3rd Cybersecurity Framework Workshop

Outbrief and Discussion of Next Steps

July 12, 2013

University of California, San Diego

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Workshop Objectives

- Discuss and Refine the draft Preliminary Framework Outline
- Generate content for the Preliminary Framework
- Discuss specific topics that inform the Preliminary Framework

What We Heard

- The Framework must support the business
- The Framework must enable cost-effective implementation
- The Framework language and communication is critical to success
- The Framework must reflect characteristics of people, processes, and technologies
- The Framework must be inclusive of and not disruptive to those good practices in use today
- The Framework must include the fundamentals
- Determination of risk tolerance for critical infrastructure must be informed by national interests
- Threat information must inform Framework implementation

Areas to Address

- Find the right level of specificity
- Threat informed
- Taxonomy for the Framework
- Identify cross-cutting categories
- Clarify the compendium of Informative References
- Integration of cyber risk into business risk
- Address IT and ICS considerations
- Framework Implementation
- Long term governance

Topic-Specific Working Sessions

- Engage senior executives and boards through effective communication of the value proposition of Framework adoption
- Provide guidance and resources to aid small business implementations
- Understand unique privacy and civil liberties needs for Critical Infrastructures
- Define awareness and training needs in context of Critical Infrastructure
- Increase international engagements
- Connect the Framework and the Performance Goals

What we will do…

- Publish a post-workshop status update
- Analyze feedback and input received this week:
  - Refine the framework structure and terminology
  - Consolidate and normalize input received
- Continue to engage with stakeholders
- Post the Draft Preliminary Cybersecurity Framework in August 2013
- Conduct the 4th Workshop at the University of Texas at Dallas (September 11-13, 2013)
- Publish the Preliminary Framework for Public Comment - October 10, 2013

Stay Engaged

Please send us your notes, continued observations, and further suggestions at cyberframework@nist.gov

Continue to work with us on populating the core framework with data

- What would sector specific representations look like?
- Identify commonalities and highlight gaps
- Share your compendiums

Review and Comment on the Next Set of Deliverables to be posted in August 2013

4th Cybersecurity Framework Workshop

September 11-13 at the University of Texas at Dallas